REMARKS

Claims 36-39 are pending herein. By this Amendment, Claims 34-35 are canceled, without prejudice or disclaimer, and new Claims 36-39 are added.

Support for the new claims is found in the specification at, *inter alia*, paragraphs [0018], [0028], [0030], [0034], [0042]-[0043], [0046], [0049], [0057], [0064], [0067], [0075], [0077]-[0078], [0088], [0090] and in the original claims. Please note that the paragraph numbers above refer to the printed patent application publication, US 2007/0005962 A1.

I. Examiner Interview

Applicant thanks Examiner Obeid and Supervisory Examiner Hewitt for the courtesies extended to Applicant and his representative at the September 2, 2009 personal interview.

At the interview, formality matters regarding canceled Claim 34 (see subject matter of new Claim 36) were first discussed, including, *inter alia*:

1) clarifying the first party computer and the second party computer;

2) changing the word "via" to "by";

3) positively reciting "partially encrypting";

4) reciting the first party computer sending the second party computer an encryption key without sending the encryption key to the broker computer (the Examiner asserted that this recitation was more preferable than reciting that the broker does not possess the encryption key);

5) clarifying that each partially-encrypted negotiating position comprises statements comprising encrypted words and non-encrypted words; and

6) reciting that the first party computer and the second party computer decode the basis-for-agreement with the encryption key.

The teachings of U.S. Patent Application Publication 2002/0184153 A1 (De Vries) and U.S. Patent No. 7,181,017 (Nagel) were then discussed. Applicant argued that De Vries requires a trusted host, i.e., a host that has the ability to decrypt information sent via a male party and a female party to determine common Interests.

Thus, De Vries does not teach or suggest (1) the first party computer sending an encryption key to the second party computer without sending the encryption key to the broker computer; or (2) the first party computer and the second party computer decoding the basis-for-agreement with the encryption key.

Nagel discloses a third party intermediary who cannot "unilaterally intercept and decrypt" information from a User and a Repository. *See* FIGS. 1-2; col. 7, lines 13-15. Applicant argued that the Intermediary is basically a key holder. In particular, Example 5 of Nagel was discussed. The User creates a message for the Data Repository. The User receives a session key from the Intermediary, computes a composite encryption key, encrypts the message, and sends it to the Repository (col. 29, lines 15-21). Once the message is sent to the Data Repository, it can never be decrypted by the User. To decrypt a message, the Data Repository communicates with the Intermediary to receive a private session key, computes a composite decryption key, and decrypts the message (col. 29, lines 22-28). In view of the extensive input of Supervisory Examiner Hewitt at the interview, his review of this Amendment would be appreciated.

II. Formal Matters

The specification was objected to as failing to provide proper antecedent basis for the claimed syntax rule.

As noted in the Amendment filed on June 2, 2009, support for the claimed "syntax rule" is found in, *inter alia*, paragraphs [0042]-[0043], paragraph [0046] (encoding rules); paragraph [0057] (predefined rules for construction of syntactically correct statements); paragraph [0072] (syntax-directed editor to follow schema); and paragraph [0090] (grammar rules). Further, there is no requirement that exact terms must be used. *See* MPEP 1302.01 noting that 37 C.F.R. 1.121(e) merely requires *substantial* correspondence between the language of the claims and the language of the specification. In addition, MPEP 2173.05(e) states:

> The mere fact that a term or phrase used in the claim has no antecedent basis in the specification disclosure does not mean, necessarily, that the term or phrase is indefinite. There is no requirement that the words in the claim must match those used in the specification disclosure. Applicants

> are given a great deal of latitude in how they choose to define their invention so long as the terms and phrases used define the invention with a reasonable degree of clarity and precision.

(emphasis added). The specification clearly provides proper antecedent basis and substantial correspondence for the claimed syntax rule. Reconsideration and withdrawal of the objection are respectfully requested.

Claims 34-35 were rejected under 35 U.S.C. 112, first paragraph, as assertedly not having an adequate written description. The rejection is respectfully traversed with respect to pending Claims 36-37.

To satisfy the written description requirement, a patent specification must describe the claimed invention in sufficient detail that one skilled in the art can reasonably conclude that the inventor had possession of the claimed invention. It is axiomatic that "[w]hile there is no *in haec verba* requirement, newly added claim limitations must be supported in the specification through express, implicit, or inherent disclosure." (MPEP 2163).

As noted above, there are numerous instances in the specification that support the claimed "syntax rule", most notably paragraph [0057] (predefined rules for construction of syntactically correct statements). Thus, Claim 36 has an adequate written description.

For pending Claim 37, please see paragraph [0078]-[0079] in US 2007/0005962 A1:

> When this optional method is employed with the invention, numerical values and value ranges are concealed by a linear mapping of values using a secret offset and secret scaling factor....To compare secret value sets, we employ the same one-way encryption key in the following way. First, the name is encrypted as a number with 2n bits. Then the high order n bits are separated from the low order bits. The two numbers of n bits are converted to an offset, a, and scaling factor, b, which are then applied to values in the value set {v1, v2, v3 . . . } producing {v1, v2*, v3* . . . } where vn*=a+b vn. The offset and scaling preserve the order relationship of the values; therefore, the values can be compared by the Broker even though the Broker does not know the original values.

(Emphasis added). Moreover, one of ordinary skill in the art would clearly understand that the Applicant was in possession of the claimed invention. Accordingly, the requirements of 35 U.S.C. 112, first paragraph, are satisfied for Claims 36-37. Reconsideration and withdrawal of the rejection are respectfully requested.

III. Rejections Under 35 U.S.C. 103(a)

Claims 34-35 were rejected under 35 U.S.C. 103(a) as unpatentable over U.S. Patent Application Publication 2002/0184153 A1 (De Vries) in view of U.S. Patent No. 7,181,017 (Nagel) and further in view of Applicant's asserted admitted prior art [***sic***: as only Claims 34-35 were pending at the time of the Office Action, it is believed that the Examiner's citation of Claims 19, 22, 25, 29, and 31 is from a previous Office Action. Further, Claim 35 is separately rejected below and the present rejection does not discuss the subject matter of that claim].

As noted above in the Examiner Interview Summary, De Vries requires a trusted host, i.e., a host that has the ability to decrypt information sent via a male party and a female party to determine common Interests. De Vries does not teach or suggest (1) the first party computer sending an encryption key to the second party computer without sending the encryption key to the broker computer; or (2) the first party computer and the second party computer decoding the basis-for-agreement with the encryption key.

Nagel does not overcome the deficiencies of De Vries. Nagel discloses a third party intermediary who cannot "unilaterally intercept and decrypt" information from a User and a Repository. *See* FIGS. 1-2; col. 7, lines 13-15. The Intermediary is a key holder. The User creates a message for the Data Repository. The User receives a session key from the Intermediary, computes a composite encryption key, encrypts the message, and sends it to the Repository (col. 29, lines 15-21). Once the message is send to the Data Repository, it cannot be decrypted by the User. To decrypt a message, the Data Repository communicates with the Intermediary to receive a private session key, computes a composite decryption key, and decrypts the message (col. 29, lines 22-28). Any combination of Nagel with De Vries would result in an inoperable method, as the trusted agent of De Vries could not function.

Further, any combination of De Vries and Nagel does not teach or suggest (1) the first party computer sending an encryption key to the second party computer without sending the encryption key to the broker computer; (2) the broker computer transmitting to the first party computer and the second party computer a basis-for-agreement comprising the statements comprising encrypted words found in both negotiating positions; and (3) the first party computer and the second party computer decoding the basis-for-agreement with the encryption key.

Further, as acknowledged by the Examiner on page 7 of the Office Action, De Vries and Nagel do not teach or suggest the broker computer identifying the syntax rule of each statement from the unencrypted words.

Applicant has not admitted that identifying a syntax rule from the unencrypted words is old and well known in the art. The subject matter of paragraph [0089] (paragraph [0090] in patent application publication, US 2007/0005962 A1) was previously discussed with the Examiner.

Applicant directed the Examiner's attention to paragraph [0015] which merely states that "it is well known that two parties can discover by encryption techniques whether they possess the same secret without revealing the secret" (i.e., through passwords to access a web server). The first sentence of paragraph [0089] merely repeats that the general process of determining the existence of a mutual shared secret is known:

> An effective method can rely on well known method to determine the existence of a mutual shared secret.

Paragraph [0089] then continues:

> **For the comparison described here** [i.e., herein in the present patent application], shared secret words are found in a semantic context established by unencrypted grammatical keywords. For example, the encrypted files can comprise structured data. By the phrase "structured data," it is meant data values that are organized in statements each of which obeys grammar rules, i.e. is a realization of rules of a production grammar. In one embodiment, structured data can comprise unencrypted keywords and encrypted vocabulary. The unencrypted keywords identify the grammatical rule for the statement while the encrypted vocabulary

> conveys the content of the statement, but only to a recipient who can decrypt the vocabulary....

(Emphasis added). When read in light of the entire specification, the meaning of paragraph [0089] is clear that a broker identifying a syntax rule from unencrypted words is a feature of the present invention. *See also* paragraph [0016] which shows the extension of the claimed method to previous methods of discovering the existence of a shared secret. Thus, it would not have been obvious for one of ordinary skill in the art to practice the claimed methods in view of the combined teachings of De Vries and Nagel. Reconsideration and withdrawal of the rejection are respectfully requested.

Claim 35 was rejected under 35 U.S.C. 103(a) as unpatentable over U.S. Patent Application Publication 2002/0184153 A1 (De Vries) in view of U.S. Patent No. 7,181,017 (Nagel) and further in view of U.S. Patent No. 7,302,582 (Snapp). This rejection is respectfully traversed with respect to pending Claim 37.

Snapp does not overcome the deficiencies of De Vries and Nagel. Snapp discloses a process of turning on bits in an array (col. 6, lines 33-53). Snapp starts with one address of 32 bits, using the 32-bit value as a "bit-address". Snapp divides a 32-bit value into high order bits and low order bits using a fixed algorithm that does not create a secret of any kind. Snapp does not teach or suggest applying linear mapping using an offset and a scaling factor to conceal the numerical values of a named set and preserve the order relationship of the numerical values. Snapp merely uses the term "offset" in the sense of an address or array position offset in hardware, not in any kind of linear mapping.

Thus, it would not have been obvious for one of ordinary skill in the art to practice the claimed methods in view of the combined teachings of De Vries, Nagel, and Snapp. Reconsideration and withdrawal of the rejection are respectfully requested.

IV. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone

interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

/Warren Zitlau/

Warren A. Zitlau, Esq.
Registration No. 39,085

CAHN & SAMUELS, LLP
1100 17th Street, NW, Suite 401
Washington, DC 20036
Telephone: (202) 331-8777
Facsimile: (202) 331-3838

Date: October 15, 2009